International Security Architects United.

Working together • Working with others • Designing security.

Standard: Defense in Depth

Date: 2022

ISAUnited
International Security Architects

/isaunited

Defense in Depth

The U.S. National Security Agency originally conceived a Defense in Depth concept and took its name from military strategy. Defense in Depth seeks to guard the population and maintain the effectiveness of defenses. Since the 1970s, it has been critical to nuclear safety. It involves establishing a series of independent lines of defense intended to prevent failures and, if prevention fails, to limit the consequences of accidents through five stages of successive safety. It was utilized in 2900 BC to Hierakonpolis in Egypt, based on a defense involving parallel and independent walls to strengthen the city's protection.

Defense in Depth uses various layers, such as fortifications, troops, and field works, instead of concentrating all resources on a single defense line. The concept is currently used for nuclear, chemical, I.T., transport, and other domains. The intent of Defense in Depth is to implement multiple and independent levels of protection (armored lines) to reduce the risk of an accidental consequence such that, if one line fails, the next will come into play in delivering the security measures necessary.

What is Defense in Depth?

Defense in Depth is a strategy that utilizes multiple safeguards to protect an organization's resources. Each safeguard is implemented to prevent an attack from causing damage. If one safeguard fails, a secondary layer of protection kicks in to minimize or avoid any negative consequences. The strategy is designed to protect the organization from a successful attack. It is not an alternative to other security strategies or tactics but rather a complementary strategy implemented in addition to the others.

How Network and Cloud Use Defense in Depth

Network and cloud use Defense in Depth by implementing multiple safeguard layers to help prevent security breaches. The following are ways network and cloud use Defense in Depth:

Control Plane Protection (Harden Network Infrastructure)

Network and cloud providers implement Defense in Depth to protect the control plane of their network infrastructure. The control plane is the part of the network infrastructure that facilitates communication between network devices and network services. This layered approach uses Defense in Depth security features, such as firewalls, intrusion detection and prevention systems (IDS/IPS), anti-malware software, secure configuration guidelines, access control lists (ACLs), packet filtering, bandwidth management tools, and global threat intelligence feeds.

Data Plane Protection (Harden Data)

Network and cloud providers implement Defense in Depth to protect the data plane of their network infrastructure. The data plane is the part of the network infrastructure that facilitates communication between network devices and network services. Cloud services typically include multiple layers (data planes) with different protocols to meet the needs of different clients better and prevent sophisticated attacks.

Endpoint Protection (Harden Stored Data)

Network and cloud providers implement Defense in Depth to protect the endpoints devices such as laptops, desktops, tablets, and smartphones. The data on these devices is protected with encryption, secure authentication, safe application listing, application control, and run-time defenses such as application behavior monitoring (ABM), vulnerability scanning, and intrusion detection systems.

Remote Access Protection (Harden Domain)

Network and cloud providers implement Defense in Depth to protect remote access users by implementing authentication, authorization, and encryption measures.

Data Classification Defense (Harden Data in Motion)

Network and cloud providers implement Defense in Depth to protect data in motion by implementing detection and prevention technologies such as firewalls, network intrusion scanning, IPS systems, anti-malware systems, data loss prevention tools, secure devices, and protocols.

Application of Defense in Depth

Defense in Depth is applied to many industries. Below are some examples of industries that use Defense in Depth:

Banks and Financial Institutions

In the financial sector and banking, Defense in Depth keeps the network and accounts safe from potential attacks. In accordance with the Payment Card Industry Data Security Standard (PCI DSS), the payment system must maintain a protected network infrastructure.

Large Companies

Defense in Depth can help large companies build a strong cybersecurity program and reduce costs by integrating detection and prevention, including firewalls, IDS/IPS security solutions, anti-malware solutions, secure device configurations and policies, and anti-phishing measures. Defense in Depth can also help these organizations better manage their risk.

Government Agencies

Defense in Depth can help government agencies, such as the Department of Defense (DoD), the Department of Homeland Security (DHS), and the U.S. Department of Veterans Affairs (V.A.), comply with specific cybersecurity requirements.

Small Businesses

Small businesses can use Defense in Depth to protect their network infrastructure and data from large-scale cyber-attacks, such as distributed denial of service (DDoS) attacks, phishing campaigns, and distributed web-based malware attacks.

Non-Profit Organizations

Defense in Depth can help non-profit organizations to comply with specific cybersecurity requirements.

Community and School Networks

Defense in Depth can help the community and school networks protect and secure their network infrastructure from unwanted access, such as via port scanning attacks, where attackers scan for publicly accessible information on a device and then use it for nefarious means.

Critical Infrastructure

Defense in Depth protects critical infrastructure, such as the electrical grid, transportation networks, and the water supply, against cyberattacks.

Benefits of Defense in Depth in Businesses

Defense in Depth provides several benefits to companies, such as:

Minimizes the Risk of An Attack Causing Damage

Defense in Depth minimizes the attack risk by implementing multiple layers of protection, such as firewall protections, IDS/IPS security solutions, anti-malware solutions, secure device configurations and policies, and anti-phishing measures.

Reduces the Cost of Cybersecurity

The cost of network and cloud cybersecurity is reduced by implementing multiple layers of protection. Since each layer effectively reduces risk, companies can implement less expensive layers and still safeguard their data.

Reduces Business Interruptions

Since Defense in Depth is a layered approach, it is used to reduce business interruption by implementing multiple safeguards that can support system downtime functions, such as data recovery, I.T. operations, and backup systems.

Increases Information Security Management Capabilities

The cybersecurity industry is complex, and it can be challenging for some organizations to manage Defense in Depth. Implementing multiple layers of protection reduces the risk of adapting to a new solution as new threats are discovered.

Increases Reputation and Cost Savings

The reputation of companies that use Defense in Depth is enhanced by implementing multiple layers of protection across their network infrastructure, applications, data centers, and remote access users. Since I.T. departments can offer their end users more sophisticated features and capabilities, business costs are reduced.

Increases Network Intelligence

Adding multiple layers of defenses can help companies uncover new security threats as they emerge. The additional layers also provide a wider range of tools and functionality used to manage the cybersecurity risk that is being managed by the organization's Defense in Depth strategy.

Conclusion

In conclusion, Defense in Depth is an effective way to protect an organization's network infrastructure and data against cyber-attacks. It is a layered approach implemented on large-scale networks, such as cloud networks. By implementing multiple layers of security, organizations can attack multiple system levels using Defense in Depth by adding new features and capabilities across their entire network infrastructure.